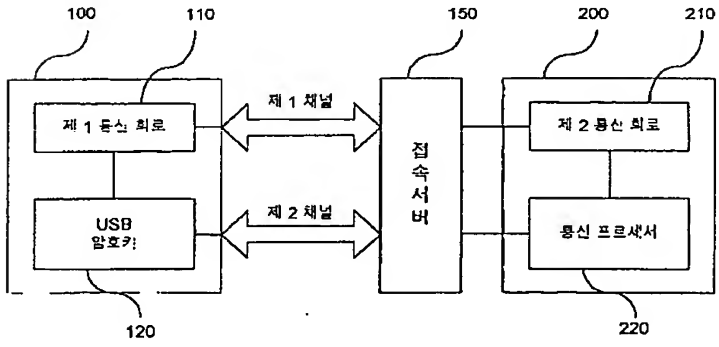
KOREAN PATENT ABSTRACTS(KR)

Document Code:A
(11) Publication No.1020010093941 (43) Publication.Date. 20011031
(21) Application No.1020000017271 (22) Application Date. 20000403
(51) IPC Code:
G06F 17/22

(71) Applicant:
LEE, SEUNG HOON
(72) Inventor:
LEE, SEUNG HOON
(30) Priority:

(54) Title of Invention
DEVICE AND METHOD FOR MANAGING ENCRYPTION KEY

Representative drawing



(57) Abstract:

PURPOSE: A device and method for managing encryption key are provided to prevent a leakage of encryption by adding an encryption function to hardware.

CONSTITUTION: A user PC(100) includes a first communication circuit(110) which processes the encryption key and a USB (universal serial bus) encryption key(120) which controls the number and time of access to a consecutive number. An access server(150) transports the encryption of the USB encryption key(120). An authentication server(200) includes a second communication circuit(210) which processes the USB encryption key(120) to make encryption text and a communication processor(220) which performs the encryption.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.		(11) 공개번호	특2001-0093941
G06F 17/22		(43) 공개일자	2001년10월31일
(21) 출원번호	10-2000-0017271		
(22) 출원일자	2000년04월03일		
---	---
(71) 출원인	이승훈 대한민국 449-843 경기 용인시 수지읍 동천리 수지2차풍림아파트 202-504
(72) 발명자	이승훈 대한민국 449-840 경기도용인시수지읍동천리수지2차풍림아파트202-504
(74) 대리인	김학제 문혜정
---	---
(77) 심사청구	있음

(54) 출원명 암호 키 관리장치 및 그 방법

요약

본 발명은 암호 키 관리장치 및 그 방법에 관한 것으로, 더욱 상세하게는 하드웨어 자체에 암호와 기능을 추가하여 암호의 유출 또는 잠재 도청자가 암호 키를 알아내지 못하도록 암호화하는 암호 키 관리장치 및 그 방법에 관한 것으로서, 본 발명에 의한 암호화 장치 및 방법에 의하면, 사용자 PC와 인증 서버간에는 암호 키를 공유할 필요가 없고 양측간의 통신에는 공개키와 암호문만이 관계하므로 암호 키가 송신되거나 공유되지 않고, 하드웨어 키와 비밀번호가 유출되는 경우에 대책을 세울 수 있으므로 우수한 결과를 얻을 수 있다.

대표도

도1

색인어

사용자 PC, 인증 서버, USB 암호 키

명세서

도면의 간단한 설명

도 1은 본 발명에 따른 암호 키 관리장치를 나타낸 블록도, 및

도 2는 도 1의 암호 키 관리 방법을 나타낸 순서도이다.

* 도면의 주요부분에 대한 부호의 설명 *

100 : 사용자 PC ○○120 : USB 암호 키

150 : 접속 서버 ○○200 : 인증 서버○○

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 암호 키 관리장치 및 그 방법에 관한 것으로, 더욱 상세하게는 하드웨어 자체에 암호화 기능을 추가하여 암호의 유출 또는 잠재 도청자가 암호 키를 알아내지 못하도록 암호화하는 암호 키 관리장치 및 그 방법에 관한 것이다.

최근 사용되고 암호화 방법 중 SSL(Secured Socket Layer)에 의한 암호화 방법은 이송 측이 암호 키로 평문(Plain Text)을 암호화하고, 그 평문을 암호문으로 변환한 후, 그 암호문을 수신 측에 전송한다. 수신 측은 대응하는 해독키로 그 암호문을 해독함으로써 암호화된 정보를 원래의 판독 가능한 형태로 변환한다.

그러나, 이 암호화 방법은 인터넷 통신상의 정보 유출에만 주안점을 두고 있기 때문에 이송 측과 수신 측이 비밀키를 생성, 공유, 저장하는 비밀번호의 관리를 복잡하게 한다. 이렇게 복잡한 관리방법은 일반 사용자들이 사용하기가 불편하기 때문에 널리 보급하는 데에는 한계가 있다는 문제가 있다.

또한, 이 암호화 방법은 만약 사용자와 서버가 인터넷에 연결된 상태(on-line)일 경우, 사용자가 인식하지 못하는 사이에 사용자의 하드웨어 키의 암호를 가로채는 키보드 훅킹(Keyboard hooking)기술을 통해 사용자가 입력한 암호가 유출될 수 있다. 즉, 암호문을 포착하여 해독하고자하는 도청자에 의하여 하드웨어 키와 비밀번호가 유출될 수 있는 문제가 있다.

발명이 이루고자 하는 기술적 과제

따라서, 본 발명은 상기와 같은 문제점을 해결하기 위해 이루어진 것으로서, 하드웨어의 간단한 조작으로 암호화 할 수 있고 도청자가 서버를 공격할 경우에 하드웨어 키와 비밀번호가 유출되는 경우에 대한 대책을 세울 수 있는 암호 키 관리장치 및 그 방법을 제공하는 데에 목적이 있다.

발명의 구성 및 작용

상기한 목적을 달성하기 위한 본 발명은, 암호 키 관리장치에 의하면, 소정의 암호 키를 처리하는 제1 통신회로와 기계적으로 장착 가능한 하드웨어키로서 일련번호를 접속한 횟수 및 그의 접속시간을 제한하도록 설치된USB 암호 키를 포함한 사용자 PC와, 상기 사용자 PC와 제1 및 제2 통신채널을 통해 접속되며 USB 암호 키의 암호를 전달하는 접속서버와, 상기 접속 서버로부터의 전달되는 암호문을 작성하고 인증하기 위해 상기 USB 암호 키를 처리하는 제2 통신회로와 암호화 처리를 위한 통신프로세서를 포함한 인증 서버를 포함한 것을 특징으로 한다.

또한 본 발명의 실시예에 따른 암호 키 관리방법에 의하면, 사용자 PC에 USB 암호 키를 삽입하는 제1 단계; 상기 사용자 PC가 접속 서버를 통해 인증 서버에 인증 서버에 접속을 요구하는 제2 단계; 상기 제2 단계에 응답하여 인증 서버는 사용자 PC로부터 받은 일련번호를 공개키로서 생성한 후, 전달하는 제3 단계; 다음, 상기 사용자 PC의 USB 암호 키는 공개키를 이용하여 암호문을 작성하는 제4 단계; 상기 작성된 암호문을 상기 USB 암호 키로부터 상기 접속 서버를 통해 상기 인증 서버에 전달하는 제5 단계; 및, 상기 인증 서버를 확인하여 상기 USB암호 키가 활성화된다면 상기 서버가 그 암호 키를 인증하는 제6 단계를 포함한 것을 특징으로 한다.

이하에서 본 발명의 암호 키 관리장치 및 그 방법의 일 실시예에 대해서 첨부된 도면 도1,및 도 2를 참조하여 설명하면 다음과 같다.

도 1은 본 발명의 실시예를 실현하는 암호 키 관리장치에 따른 사용자 PC(100), 접속서버(150), 및 인증 서버(200)를 갖는 회로 노드의 구조를 도시한 블럭도이다. 도시된 실시예에서 사용자 PC(100)는, 제1통신회로(110), 상기 사용자 PC(100)내에 삽입가능한 USB(Universal Serial Bus)암호 키(120)로 구성되어 있다. 또한 네트워크 센터의 인증 서버(200)는 제2 통신회로(210)와 통신 프로세서(220)로 구성되어 있다. 상기 사용자 PC(100)의 제1 통신회로(110)는 소정의 암호 키를 처리하는 역할을 한다. 상기 USB 암호 키(120)는 상기 사용자 PC(100)에 기계적으로 장착 가능한 하드웨어 키로서의 역할을 한다. 상기 접속서버(150)는 상기 사용자PC(100)와 인증 서버(200)사이에서 암호 키를 관리하는 에이전트 역할을 한다. 상기 인증 서버(200)의 제2 통신회로(210)와 통신프로세서(220)는 상기 접속 서버(150)와 연결되고 상기 USB암호 키(120)에 대하여 인증하는 역할을 한다. 상기 인증 서버(200), 상기 접속 서버(150), 및 사용자 PC(100)는 통상 통신 네트워크내의 떨어진 위치에 배치된다. 선택적으로 접속 서버(150)는 상기 인증 서버(200)내에 장착될 수도 있다. 상기 사용자 PC(100)의 USB 암호 키(120)는 엄쇠고리 크기 정도의 크기를 가진다. 또 상기 USB 암호 키(120)는 각 제조회사의 생산 공정에서, 고유의 일련 번호를 암호화한 암호문이 등록되어 있고, 소정의 암호화 회로가 내장되어 있다.

상기 USB 암호 키(120)는 셀러론 CPU 또는 펜티엄 CPU 이상을 장착한 PC에 장착되는 포트로서 핫 플러그 인(Hot Plug-in)과 플러그에 따른 플레이가 가능하며, 선택적으로 네트워크 인증 서버 시스템에도 적용가능하다.

도 1에 있어서, 사용자 PC(100)는 내부의 제1 통신회로(110)에서 USB암호 키(120)를 거쳐서 인증 서버(200)내부의 제2 통신회로(210)로 제1의 일련번호를 송신한다. 여기서 USB 암호 키(120)의 일련번호는 8내지 10디지트의 시퀀스 길이를 포함한다. 이 USB 암호 키(120)의 일련번호는 제1 통신 채널을 통해 상기 접속 서버(150)로 송신된다. 통신 네트워크 센터 시스템내의 인증 서버(200)는 상기 접속 서버(150)로부터의 접속이 허용되면, 상기 USB암호 키(120)내에서 USB 암호 키(120)의 일련번호를 수신하여 저장한다. 다음에 인증 서버(200)는 제2 통신회로(210)에서 USB 암호 키(120)로 제2채널을 통해 일련 번호를 수신하여 저장한다.

본 발명의 암호화 관리 장치는 도청자 서버의 공격에 대한 USB 포트 키(120)의 일련번호 자체를 암호화한다. 또한, 비록 암호 체계가 파악되더라도 도청이 곤란하도록, 인증 서버(200)에 일련번호를 전송한 횟수를 삽입한다. 또 암호체계의 복제 및 파악을 위한 시도 자체도 어렵게 하기 위해 한번 접속한 뒤 다음 접속 시까지 일정한 시간 간격을 둔다. 그리고 이러한 일정시간에 시도 할 수 있는 조회 횟수를 제한한다. 이에 의하여, 입력 횟수의 입력 초과 또는 일정한 시간간격, 또는 조회횟수의 초과가 있게되면, 이미 저장된 암호 데이터를 삭제하여 더 이상의 접속시도가 불가능하게 한다.

또한 USB 포트(120)의 속도와 하드웨어 키의 처리시간으로 인해 한번 확인한 시간이 더욱 길어지므로 하나의 비밀번호를 찾아 확인하는데 필요한 절대 시간을 길게 할 수 있어 암호 키의 보안성을 향상시킨다.

이제, 도 2를 참조하면, 본 발명의 실시예에 따라 무선 통신 네트워크에서 암호 키를 발생시키는 흐름도가 도시되어 있다.

초기화 스텝에서 사용자는 가정이나 사무실의 통신선으로부터 가입자센터의 인증 서버(200)로 통신선의 호출을 한다. 이때 사용자 PC(100)는 시동되었지만 여전히 비작동 상태이다. 그후 사용자가 그의 PC(100)에 USB암호 키(120)를 삽입한다(스텝 1). 이 때 사용자가 그의 암호를 사전에 입력한다.

상기 스텝1 의 상태에서 사용자 PC(100)가 USB 암호 키(120)를 통해 접속 서버(150)에 접속을 요구한다(스텝 3). 이에 응답하여 접속 서버(150)는 사용자 PC(100)의 USB 암호 키(120)로부터 받은 일련번호를 전달한다. 상기 전송된 일련번호는 인증 서버(200)의 제2 통신회로(210)에서 공개키를 생성한다. 그리고 인증 서버(200)내 통신 프로세서(220)의 제어 하에 제2 통신회로(210)가 상기 공개키를 이용하여 접속서버(150)를 통해 USB 암호 키(120)에 전달한다(스텝 5).

그후, USB 암호 키(120)는 상기 제2 통신회로(210)로부터 전송된 USB공개키(120)를 해독하고 새로운 암호문을 작성한다(스텝 7). 이때 사용자 PC(100)의 USB 암호 키(120)는 인증 서버(200)에서 받은 키와 인증 서버(200)에 보낸 횟수를 이용하여 암호화한다. 여기서, USB암호 키(120)내에 저장된 정보는 항상 사용자에 의해 암호문으로 변환되어 저장된다. 그후, 사용자 PC(100)는 이 암호문을 접속 서버(150)를 통해 인증 서버(200)에 전달한다(스텝 9). 여기서, 인증 서버(200)에 접속 시에는 USB 암호 키(120)에 전달된 공개키를 이용하여 사용자의 입력에 의해 암호가 해제된 일련번호를 다시 암호화하여 인증 서버(200)에 전달할 수 있다.

그후 인증 서버(200)는 암호문이 정당한 것 인지의 여부를 확인하고(스텝 11), 일련번호의 접속횟수를 확인하여 USB암호 키(120)가 활성화된다면 그 암호 키(120)를 인증하고(스텝 13), 그렇지 않다면 접속을 거절한다(스텝 15).

발명의 효과

따라서 본 발명에 의한 암호화 장치 및 방법에 의하면, 사용자 PC와 인증 서버간에는 암호 키를 공유할 필요가 없고 양측간의 통신에는 공개키와 암호문만이 관계하므로 암호 키가 송신되거나 공유되지 않는다. 결국, 하드웨어 키와 비밀번호가 유출되는 경우 또는 서버 공격이 있을 경우에 대책을 세울 수 있으므로 우수한 결과를 얻을 수 있다.

본 발명의 실시예는 예시의 목적을 위한 것으로, 이 기술분야에서 통상의 지식을 가진 자라면, 본 명세서에 예시된 기술적 범위를 통해 수정, 변경, 대체 부가가 가능할 것이다.

(57) 청구의 범위

청구항 1.
암호 키 관리장치에 있어서,

소정의 암호 키를 처리하는 제1 통신회로와 기계적으로 장착 가능한 하드웨어키로서 일련번호를 접속한 횟수 및 그의 접속시간을 제한하도록 설치된USB 암호 키를 포함한 사용자 PC와,

상기 사용자 PC와 제1 및 제2 통신채널을 통해 접속되며 USB 암호 키의 암호를 전달하는 접속서버와,

상기 접속 서버로부터의 전달되는 암호문을 작성하고 인증하기 위해 상기 USB 암호 키를 처리하는 제2 통신회로와 암호화 처리를 위한 통신프로세서를 포함한 인증 서버를 포함한 것을 특징으로 하는 암호 키 관리장치.

청구항 2.
제 1항에 있어서, 상기 사용자 PC의 USB 암호 키는 고유의 일련 번호와 암호가 입력된 암호화 회로를 포함한 것을 특징으로 하는 암호 키 관리장치.

청구항 3.
사용자 PC에 USB 암호 키를 삽입하는 제1 단계;

상기 사용자 PC가 접속 서버를 통해 인증 서버에 인증 서버에 접속을 요구하는 제2 단계;

상기 제2 단계에 응답하여 인증 서버는 사용자 PC로부터 받은 일련번호를 공개키로서 생성한 후, 전달하는 제3 단계;

다음, 상기 사용자 PC의 USB 암호 키는 공개키를 이용하여 암호문을 작성하는 제4 단계;

상기 작성된 암호문을 상기 USB 암호 키로부터 상기 접속 서버를 통해 상기 인증 서버에 전달하는 제5 단계; 및,

상기 인증 서버를 확인하여 상기 USB암호 키가 활성화된다면 상기 서버가 그 암호 키를 인증하는 제6 단계를 포함한 것을 특징으로 하는 암호 키 관리방법.

청구항 4.
제3 항에 있어서,

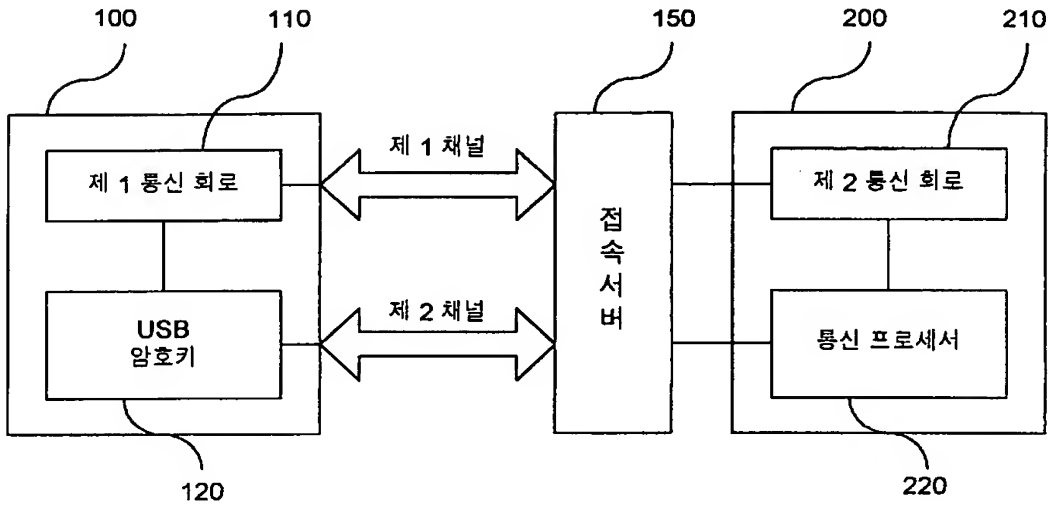
상기 제4 단계에서 상기 제2 통신회로에서 전송된 암호문을 해독하는 제7 단계를 포함한 것을 특징으로 하는 암호 키 관리방법.

청구항 5.
제3 항에 있어서,

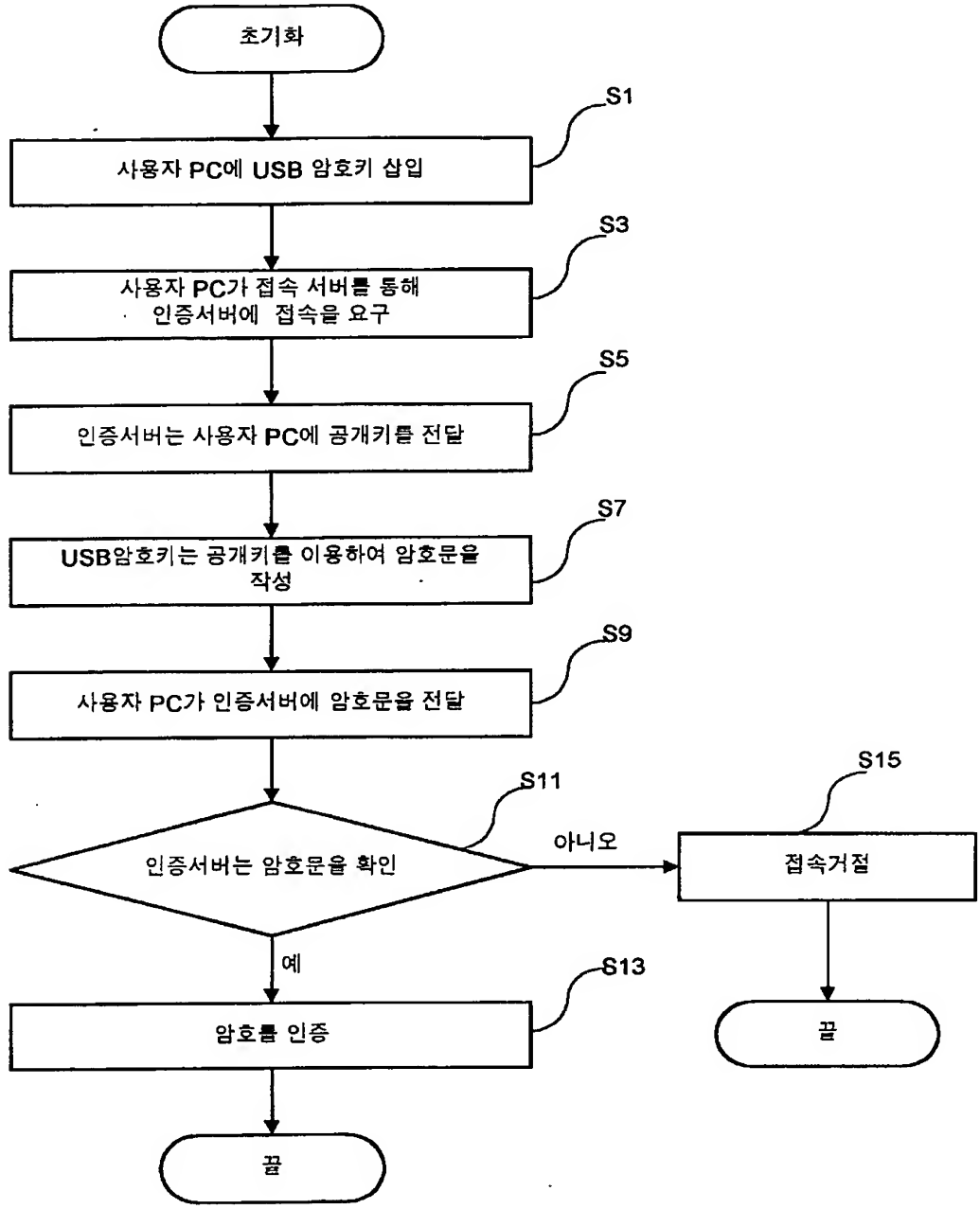
상기 제6 단계에서 확인하여 암호 키가 활성화되지 않다면 접속을 거절하는 하는 제8 단계를 포함한 것을 특징으로 하는 암호 키 관리방법.

도면

도면 1


100
110
150
200
210
제 1 통신 회로
제 1 채널
제 2 통신 회로
접속서버
USB 암호키
제 2 채널
통신 프로세서
120
220

도면 2


초기화
S1
사용자 PC에 USB 암호키 삽입
S3
사용자 PC가 접속 서버를 통해
인증서버에 접속을 요구
S5
인증서버는 사용자 PC에 공개키를 전달
S7
USB암호키는 공개키를 이용하여 암호문을
작성
S9
사용자 PC가 인증서버에 암호문을 전달
S11
인증서버는 암호문을 확인
아니오
S15
접속거절
끝
예
S13
암호를 인증
끝